Lab Director

SUBJECT: SAFEGUARDS AND SECURITY SURVEY OF (Facility Name), Inspection Dates

The subject Safeguards and Security Survey will be conducted in accordance with the requirements of Department of Energy Order 470.4 and will involve a review and evaluation of (FACILITY NAME)'s Safeguards and Security Program. This survey will address the following topical areas, and be conducted by the following DOE and support personnel:

- Program Management and Support
- Protective Force
- Physical Security
- Information Protection
- Cyber Security
- Personnel Security Program
- Unclassified Visits and Assignments by Foreign Nationals
- Nuclear Materials Control and Accountability

(Insert name of Survey Team Leader) will serve as team leader for this survey. A list of documentation required by the survey team is enclosed. All items indicated in **bold** should be provided to (Surveying Office) Safeguards and Security Services (Attention: Survey Team Leader) by (date). The survey in briefing is tentatively scheduled for (date and time). The remaining items in the data call should be available for review by the team members on the first date of the survey.

All survey team members will possess appropriate access authorization and presentation of their badges/credentials will suffice to authorize their access to any information pertinent to the survey. Please ensure that the appropriate members of your staff are available in order for the survey to be completed in the allotted time. Interaction between the survey team, (Facility Name) management, and the (Name of Facility's Site Office Pacific) management will be maintained throughout the inspection process to assure that any areas of concern are communicated and discussed as they develop.

If you have any further questions, please contact (typically a Site Office person or Lab Personnel) at (Phone Number).

Sincerely,

Enclosure:
As Stated

Integrated Safeguards and Security Survey
(Facility Name)
(Survey Dates)

Data Call

***Items in bold should be provided to Surveying Office by (date).**

Program Management and Support

1. **An organization and function chart to include all Safeguards and Security (S&S) personnel (Management, Staff and Administrative). The list should reflect each person's S&S function(s), duties and responsibilities (job title); level of access authorization and entry on duty date.**

2. A list of all current, approved job analysis (JA's) for S&S employees, their completion date, their Chicago approval date, their review date and projected review & completion date for any JA changes.

3. A list documenting any and all S&S training programs, lesson plan titles for each, and a task to training matrix for each.

4. All S&S personnel training records.

5. **A copy of the S&S Self Assessment Plan, the results of all Self Assessments conducted during the past 12 months and the status of corrective actions for noted deficiencies.**

6. Documentation concerning all S&S related reportable occurrences and all Security Infractions/Violations for the past 12 months.

7. A copy of procedures for establishing security interests and submitting Contract Security Classification Specification forms.

8. A list of all contracts or purchase agreements involving access to classified matter, significant quantities of Special Nuclear Material, or the granting of Access Authorizations that have been executed in the past 12 months.

9. **A list of all S&S related plans (including drafts). This list should include title, approval date (submission date for drafts), area/location to which the plan is applicable, and authorized activities (e.g., storage, generation).**

10. The most recent edition of the Training Approval Program Assessment Report.

11. A copy of procedures for the implementation of Foreign Ownership Control and Influence (FOCI) requirements.

12. **Spreadsheet listing all Safeguards and Security related reportable Incidents of Concerns and if a Security Infractions/Violations was issued for the past 24 months. Actual Inquiry reports should be made available during the survey.**

13. Examples of Inquiry appointment letters, and training profiles. Additional files should be available during the survey.

Protective Force (PF)

1. All Memorandums of Understanding or Memorandums of Agreement the Lab has concerning PF issues.

2. A list of all posts and patrols, location of their corresponding orders, and a copy available to the inspection team.

3. Have available any performance testing documentation for the last 12 months.

4. **Follow-up/investigative reports for inventory shortages, property loss, property theft, or missing property for the last Fiscal Year.**

Physical Security

1. **A list of all badges and passes issued, stored, lost or stolen, reissued and retrieved at the time of separation.**

2. Procedures for requesting maintenance for security systems.

3. Testing records for the last year for security systems and components, including the uninterruptible power sources (e.g., battery, emergency generator), including frequency of testing.

4. Available for review – Test procedures, including frequency of testing for security systems components (e.g., alarm sensors, tamper capabilities, and auxiliary power systems.)

5. Documentation detailing all changes in alarm systems (including computer software) since the last security survey. This should include a description in place to ensure changes are correctly implemented and that no unauthorized changes have occurred.

6. A list of all incoming alarms for the week of (date).

7. Up-to-date floor plans for all Special Nuclear Material, classified matter, and property protection areas.

Information Protection

Classification

1. A list of all Classification personnel to include Derivative Classifiers (DC), Derivative Declassifiers (DD), and Administrative Staff. The list should indicate each person's job title, DC or DD, and appointment authority.

2. List of all HQ and locally approved classification guides. The location and individual's name issued to the above guides.

3. Appointment letters of all Classification personnel (including Classification Officer [CO], DC, DD, Reviewing Official).

4. **A copy of the corrective actions implemented for any findings issued within the last 24 months.**

5. Make available a copy of CO's position description, and evaluations identifying critical skills. If others are evaluated as a critical performer, please also include.

6. Statistics for the last 24 months of classification & declassification activities.

7. Make available a sampling of all approved DOE Forms 470.1 and security interests generating classified matter.

8. Any approved, or applied for deviation from DOE Manual 475.1-1A for the last 24 months.

9. Any Declassification Initiatives completed or continuing for the last 24 months.

10. Copy of latest classification program related training materials.

Classified Matter Protection and Control (CMPC)

1. **Current (FACILITY NAME) Organization Chart, with identified Information Protection, CMPC and Classification function identified.**

2. **A list detailing all Security Areas (including temporary, Limited Area's, or higher, if any). Include information for the points of contact, approved area activities/functions.**

3. **A list of all Security Containers (including Vault Type Rooms and Vaults) and there location by building and room. Any containers that store accountable matter should be further identified by matter type.**

4. **A listing of the total number of classified documents/hardware (if any) by level, category by division.**

5. A list of all control stations locations. Please include all approved control station operators appointment letters.

6. A list of personnel authorized to: receive matter addressed to the classified mailing address; prepare classified documents for transmittal; and access classified matter repositories.

7. A listing of all individuals approved by to Hand Carry classified matter within the last 24 months.

8. **Copies of all classified document inventories conducted in the last 24 months (Including Accountable Classified Removable Electronic Media [ACREM] activities).**

9. A sample copy of accountability log, destruction log, incoming and outgoing mail logs, or any other site specific log used within the CMPC program.

10. A copy of the latest CMPC program related training materials specifically ACREM, CMPC related Custodian, and Refresher training/ briefings.

Classified Cyber Security/Telecommunications Security

1. **Inventory by location of classified systems both hardware and software components to include identification of classified facsimile systems or systems that use secure communications equipment (Secure Telephone Equipment [STE] phones and modems).**

2. Copies of accreditation letters and annual security certification tests for the last 12 months.

3. A copy of the Diskless Workstation Task Force conversion plan.

4. User training records for the most recent training session conducted and copies of User Code of Conduct documentation.

5. A copy of training attendance records for the past 12 months for the Information Security Site Officer (ISSO), Information Security Site Manager (ISSM) and classified system users.

6. **Copies of reports of internal and external audits and compliance reviews related to the classified computer security program conducted in the past 12 months. Provide a summary of corrective actions taken regarding findings and recommendations from those reviews.**

7. Copies of appointment letters for the ISSM and the ISSO.

8. **A copy of incident reporting procedures along with any incident reports within the past 12 months.**

9. **A copy of the site's self and risk assessment for the Classified Information Systems Security Program.**

10. A copy of the annual TEMPEST review for the laboratory.

11. A copy of the CDIN plan for appropriate systems (e.g. SIPRNET).

Unclassified Cyber Security

1. **A summary of site computing resources to include networks, host systems, subnets (including a summary of the clients on each subnet), routers, switches, firewalls, and other boundary devices (bridges, proxies, network address translation devices, etc.). This summary should include: a listing of defined cyber enclaves (with a description of the enclave and the name and telephone number of the enclave point**

the enclave point of contact), a diagram of the network architecture; the range of registered Internet Protocol (IP) addresses; the IP address range of major networks and subnets; firewall type and rules; router types and rules, access control lists; description of all connections to the public and DOE networks; a list of internal IP addresses; a summary of trust relationships (both internal and external); and a list of authorized modems with location and telephone number.

2. **Security Certification documentation for each Cyber enclave. This should include the following:**
3. **The current site Cyber Security Program Plan and Risk Assessment.**
4. **Security plans, supplemental risk assessments and contingency plans for each cyber enclave.**
5. The authority to operate letters for each enclave to include documentation of residual risks accepted by the Designated Accrediting Authority.
6. Security Testing and Evaluation results for each cyber enclave.
7. Status of corrective actions for all Plan of Action and Milestones items, including those from the Office of Science Site Assistance Visit.
8. Identification of all OMB Exhibit 53 and Exhibit 300 systems included in each enclave.
9. A description of each wireless network installation to include location, purpose, area of coverage, connectivity to the site network infrastructure, and the name and telephone numbers of staff responsible for operations and security.
10. **Approved performance testing agreement with a list of any times that performance testing may not take place and a complete list and justification of systems that are not to be scanned.**
11. **A copy of site security policies that are used to develop firewall rules, intrusion detection architecture and system parameters.**
12. **A copy of security policies and rules for remote access to network systems and resources.**
13. A copy of the results of the most recent self-assessment of the cyber security program and documentation of network security testing conducted in the last 24 months.
14. Documentation of all cyber security incidents and investigations during the last 24 months.

Personnel Security

1. **A copy of Standard Operating Procedures for Personnel Security Program.**

2. **Self-Assessment for the Personnel Security Program.**

3. **A list of all Security Education briefings conducted since (date) by type of briefing (e.g., initial, comprehensive, refresher, and termination) name, and date of briefing.**

4. **A list of all cleared employees who are or have been absent from work for more than 90 days (e.g. leave, assignment, extended travel). The list should include name, position, clearance number and dates of absence.**

5. **A list of all employees or consultants holding an access authorization. Indicate those individuals whose duties actually require access to classified matter, an exclusion area, or significant quantities of Special Nuclear Material.**

6. **A copy of Standard Operating Procedures for the Classified Visit Program.**

7. **A list of individuals requesting a classified visit, name of host and type of information requested and type of information accessed.**

8. **A list of all new hires since (date).**

9. **A list of all employees terminated since (date). List will include name, clearance number and date of termination.**

10. **A list of Special Term Appointee(s), level of clearance(s), and the last time classified was accessed.**

11. A current list of all employees with access to Sensitive Compartmented Information and Weapons Data.

<u>Unclassified Visits and Assignments by Foreign Nationals</u>

1. Specific Security Plans and IA-593s, as well as a record of indices checks and Visitor Registration Logs applicable to such visits since January 2005.

2. A list of foreign visitors that required an export License.

3. **Standard Operating Procedures for the Foreign Visits and Assignments Program to include Export Control Procedures.**

4. **A list of all site Visits/Assignments by Foreign Nationals to (FACILITY NAME) since (date), to include those foreign nationals from Terrorist-sponsored countries. Documentation is to include the visitor's name, country of birth, country of citizenship, visit/work area(s) on site, beginning and ending date of visit/assignment.**

5. **A copy of Self-Assessment for the Foreign Visits and Assignments Program.**

6. **A copy of Sensitive Subjects List.**

7. Documentation concerning reportable security incidents which involves foreign nationals, illegal drugs, alcohol and security infractions.

Nuclear Material Control and Accountability

1. **Copies of all occurrence reports involving nuclear materials in the last 12 months. Please include documentation of all follow-up activities.**

2. **A current listing of all areas authorized for the use and storage of nuclear materials. Include the names of the custodians and alternates and a brief description of the area.**

3. **One set of nuclear material inventory listings for the site as of (date).**

4. **A list of all internal and external nuclear material transfer documents for the period (date) through (date).**

5. **A list of all measurement systems qualified for accountability purposes including precision and accuracy requirements for each measurement technique.**

6. All accountability ledgers (manual and automated), documents, and procedures should be available to team members during the inspection**.**